CLAIMS

What is claimed is:

1   1.   Embodied in a memory component, a digitally signed image comprising:

2   a post-relocation image being an image of a software module altered by a

3   symmetrical relocation function upon loading of the image into the memory component;

4   and

5   a digital signature based on the image.

1   2.   The digitally signed image of claim 1, wherein the digital signature is a

2   hash value of the image digitally signed by a private key of a selected signatory.

1   3.   The digitally signed image of claim 1 further comprising information for

2   use by the symmetrical relocation function to convert the image into the relocation image.

1   4.   The digitally signed image of claim 3, wherein the information includes

2   offsets for routines within the software module.

1   5.   The digitally signed image of claim 4, wherein the offsets are generated

2   when the software module is compiled.

1   6.   Embodied in a memory component, a digitally signed image comprising:

2   a Bound & Relocated Import Table (BRIT);

3   an import table;

4   an export table;

5   an image of a software module; and

6   a digital signature based on the import table, the export table and the image.

1   7.   The digitally signed image of claim 6, wherein the import table comprises

2   a plurality of entries, each entry includes an identifier that indicates what segment of

3   information contained in another digitally signed image is required by the image.

1   8.   The digitally signed image of claim 7, wherein the identifier includes a

2   unique sequence of byte values.

1   9.   The digitally signed image of claim 7, wherein the identifier includes a

2   unique sequence of alphanumeric characters.

1   10.   The digitally signed image of claim 7, wherein each entry of the import

2   table further includes an offset to a corresponding entry of the BRIT.

1   11.   The digitally signed image of claim 6, wherein the export table includes a

2   plurality of entries forming a listing of segments of information contained in the image, a

3   selected entry of the plurality of entries includes an identifier of a segment of information

4   associated with the segments of information.

1   12.   The digitally signed image of claim 11, wherein the selected entry further

2   includes a second offset being an offset from a starting address of the digitally signed

3   image to an address location of the segment of information.

1   13.   A method comprising:

2   reconverting a post-relocation image of a digitally signed image back to a pre-

3   relocation image, the pre-relocation image being an image of a software module prior to

4   be altered by a symmetrical relocation function;

5   conducting a hash operation on the reconverted, pre-relocation image to produce a

6   reconverted hash value;

7   recovering a hash value from a digital signature contained in the digitally signed

8   image, the hash value is based on the image of the software module; and

9   comparing the hash value to the reconverted hash value.

1   14.   The method of claim 13 further comprising:

2   determining that an integrity of the post-relocation image remains intact if the

3   hash value matches the reconverted hash value.

1   15.   The method of claim 13 further comprising:

2   determining that the post-relocation image has been modified beyond any

3   modification caused by relocation when the hash value fails to match the reconverted

4   hash value.

1   16.   The method of claim 13, wherein the hash operation is a one-way hash

2   operation.

1   17.   A method for generating a Bound & Relocated Import Table (BRIT)

2   within an electronic device, comprising:

3   (a) locating an import table for a first digitally signed image loaded within the

4   electronic device, each entry of the import table including an identifier and a first offset;

5   (b) accessing an identifier within a selected entry of the first digitally signed image;

6   (c) determining whether the identifier matches an identifier within an export table

7   of a second digitally signed image loaded within the electronic device, the identifier for

8   the export table is stored with a corresponding second offset; and

9   (d) upon determining that the identifier within the selected entry matches the

10   identifier within the export table,

11   producing an address by combining the second offset with a starting

12   address of the second digitally signed image, and

13   loading the identifier within the selected entry and the address into an

14   entry of the BRIT.

1   18.   The method of claim 17 further comprising:

2   repeating the operations of (a)-(d) for each remaining entry of the import table for

3   loading resultant address and identifier pairs into different entries of the BRIT.

1   19.   The method of claim 17, wherein the producing of the address by

2   combining the second offset with the starting address of the second digitally signed image

3   comprises an arithmetic operation.

1   20.   The method of claim 17, wherein prior to locating an import table for the

2   first digitally signed image, the method further comprises locating a plurality of digitally

3   signed images loaded within the electronic device.

1   21.   A method comprising:

2   verifying an integrity of a plurality of digitally signed images loaded in an

3   electronic device, the plurality of digitally signed images includes a first digitally signed

4   image and a second digitally signed image;

5   determining whether an identifier in an import table of the first digitally signed

6   image matches an identifier in an export table of the second digitally signed image; and

7   determining whether an entry of a Bound & Relocated Import Table (BRIT)

8   corresponding to the identifier in the import table points to an address defined by the

9   identifier in the export table.

1   22.   The method of claim 21, wherein the verifying the integrity of the plurality

2   of digitally signed images includes

3   performing a hash operation on the import table, the export table and an image of

4   the first digitally signed image to produce a first resultant hash value;

5   recovering a first hash value from a digital signature contained in the first digitally

6   signed image; and

7   comparing the first hash value with the first resultant hash value.

23. The method of claim 22, wherein the verifying the integrity of the plurality

of digitally signed images further comprises

performing a hash operation on an import table, an export table and an image of

the second digitally signed image to produce a second resultant hash value;

recovering a second hash value from a digital signature contained in the second

digitally signed image; and

comparing the second hash value with the second resultant hash value.

24. An electronic device comprising:

a processor; and

a non-volatile memory component in communication with the processor, the non-

volatile memory component includes including

a post-relocation image being an image of a software module altered by a

symmetrical relocation function upon loading of the image into the memory

component, and

a digital signature based on the image.

25. The electronic device of claim 24, wherein the non-volatile memory

component further includes information for use by the symmetrical relocation function to

convert the image into the post-relocation image.

26. The electronic device of claim 25, wherein the information placed within

the non-volatile memory component includes offsets from a starting address of the image

of the software module to a segment of information within the software module.

27. An electronic device comprising:

a processor; and

a memory in communication with the processor, the memory being loaded with a

Bound & Relocated Import Table (BRIT), an import table, an export table, an image of a

5 software module, and a digital signature based on the import table, the export table and
6 the image.

1   28.   The electronic device of claim 27, wherein the import table loaded within
2 the memory comprises a plurality of entries, each entry includes an identifier that
3 indicates what segment of information contained in another digitally signed image is
4 required by the image.

1   29.   The electronic device of claim 28, wherein the identifier associated with a
2 particular entry includes a unique sequence of byte values.

1   30.   The electronic device of claim 27, wherein the export table includes a
2 plurality of entries forming a listing of segments of information contained in the image, a
3 selected entry of the plurality of entries includes an identifier of a segment of information
4 associated with the segments of information.

1   31.   Embodied in a processor readable medium for execution by a processor, a
2 software program comprising:
3   a first software module to reconvert a post-relocation image of a digitally signed
4 image back to a pre-relocation image, the pre-relocation image being an image of a
5 software module prior to be altered by a symmetrical relocation function;
6   a second software module to conduct a hash operation on the reconverted, pre-
7 relocation image to produce a reconverted hash value;
8   a third software module to recover a hash value from a digital signature contained
9 in the digitally signed image, the hash value is based on the image of the software
10 module; and
11   a fourth software module to compare the hash value to the reconverted hash value.

1   32.   The software program of claim 31 further comprising:
2   a fifth software module to determine that an integrity of the post-relocation image
3 remains intact if the hash value matches the reconverted hash value.

1   33.   The software program of claim 31 further comprising a sixth software

2   module to determine that the post-relocation image has been modified beyond any

3   modifications caused by relocation when the hash value fails to match the reconverted

4   hash value.